

Home Digital Safety Baseline Checklist

Use this checklist to verify the basics at your own pace. A checked box means **you verified it** - it does not mean TechSprouthQ tested your account or device.

PDF version: 1.0	Last reviewed: September 19, 2026
Full guide: techsprouthq.com/home-digital-safety-baseline/	Evidence: Companion checklist

Keep your progress: The web checklist does not save checked boxes after the page reloads. Use this PDF if you want a copy you can print, annotate, or save locally.

Start with the accounts and devices that would cause the biggest problem if you lost access to them. Then work through the rest.

PRIMARY EMAIL

- ☐ My primary email uses a password I do not use anywhere else.
- ☐ MFA or a passkey is enabled on my primary email.
- ☐ My recovery email address and recovery phone number are current.
- ☐ I removed old devices or recovery methods I no longer control.
- ☐ I know how I would recover my email if I lost my phone.

MOBILE-CARRIER ACCOUNT

- ☐ My carrier account has a strong, unique PIN or password.
- ☐ The email tied to my carrier account is secure and current.
- ☐ I checked whether my carrier offers a number lock, port-out lock, SIM-change lock, or similar protection.
- ☐ I know how to contact my carrier from another device if my phone unexpectedly loses service.

PASSWORDS

- ☐ I use a reputable password manager or another system that gives important accounts genuinely different passwords.
- ☐ My password manager, if used, has a strong master password or passphrase that is not reused.
- ☐ Reused passwords have been replaced on my highest-impact accounts first.

MFA / PASSKEYS

- ☐ MFA is enabled on my most important accounts.
- ☐ I use a passkey, security key, or authenticator app instead of SMS where a stronger option is practical and supported.
- ☐ Recovery codes are stored somewhere safe and separate from my normal sign-in device.
- ☐ Old authenticators or phones I no longer control have been removed.
- ☐ I know not to give an unexpected caller or texter a verification code.

DEVICES

- ☐ Automatic operating-system updates are enabled.
- ☐ Browser and app updates are enabled or regularly installed.
- ☐ Phones, tablets, and computers use a screen lock.
- ☐ I checked whether device or disk encryption is enabled.
- ☐ I know where encryption recovery information is stored, if my device uses it.

HOME WI-FI

- ☐ My router or mesh administrator password is not the factory default.
- ☐ My Wi-Fi password is strong and not reused as an account password.
- ☐ Wi-Fi security is set to WPA3 Personal or WPA2 Personal.
- ☐ Router or mesh firmware is current or automatic updating is enabled.
- ☐ Remote management is disabled if I do not use it.
- ☐ I log out of the router administrator interface when I am finished.

BACKUPS

- ☐ Important files have at least one additional copy.
- ☐ I know whether the backup is local, cloud, or both.
- ☐ I checked what my cloud or sync service can actually restore.
- ☐ I know how to start a restore.
- ☐ I successfully restored at least one harmless test file.

PHISHING / UNEXPECTED MESSAGES

- ☐ Household rule: an unexpected message does not get to choose the link, phone number, or sign-in page we use to verify a problem.
- ☐ I know how to reach important companies through an app, website, or phone number I already trust.
- ☐ I do not give unexpected callers or texters passwords, MFA codes, or remote access.

HOUSEHOLD RECOVERY MAP

- ☐ A recovery map exists.
- ☐ The map records where recovery starts without storing passwords, MFA codes, recovery keys, bank account numbers, or other secrets.
- ☐ The baseline has a review date.

Last reviewed: _____

NEXT REVIEW TRIGGER

Review this baseline again after a major phone or computer replacement, password-manager change, router replacement, backup change, account compromise, mobile-carrier change, or another meaningful household technology change.

Locations only - no secrets

IMPORTANT: Do not write passwords, MFA codes, recovery keys, account numbers, Social Security numbers, or other sensitive secrets on this checklist. This is a process map, not a secret vault.

Primary recovery email provider:

Password manager used:

Recovery codes are stored at:

Mobile carrier portal:

Carrier number-lock / port-protection status:

Family photo / important-file backup service:

Offline or external backup location:

Home router / mesh system:

Device-encryption recovery information is stored at:

Other important recovery starting point:

The recovery map should tell someone where recovery starts - for example, which provider, portal, device, or physical location to use - without containing the secret itself.